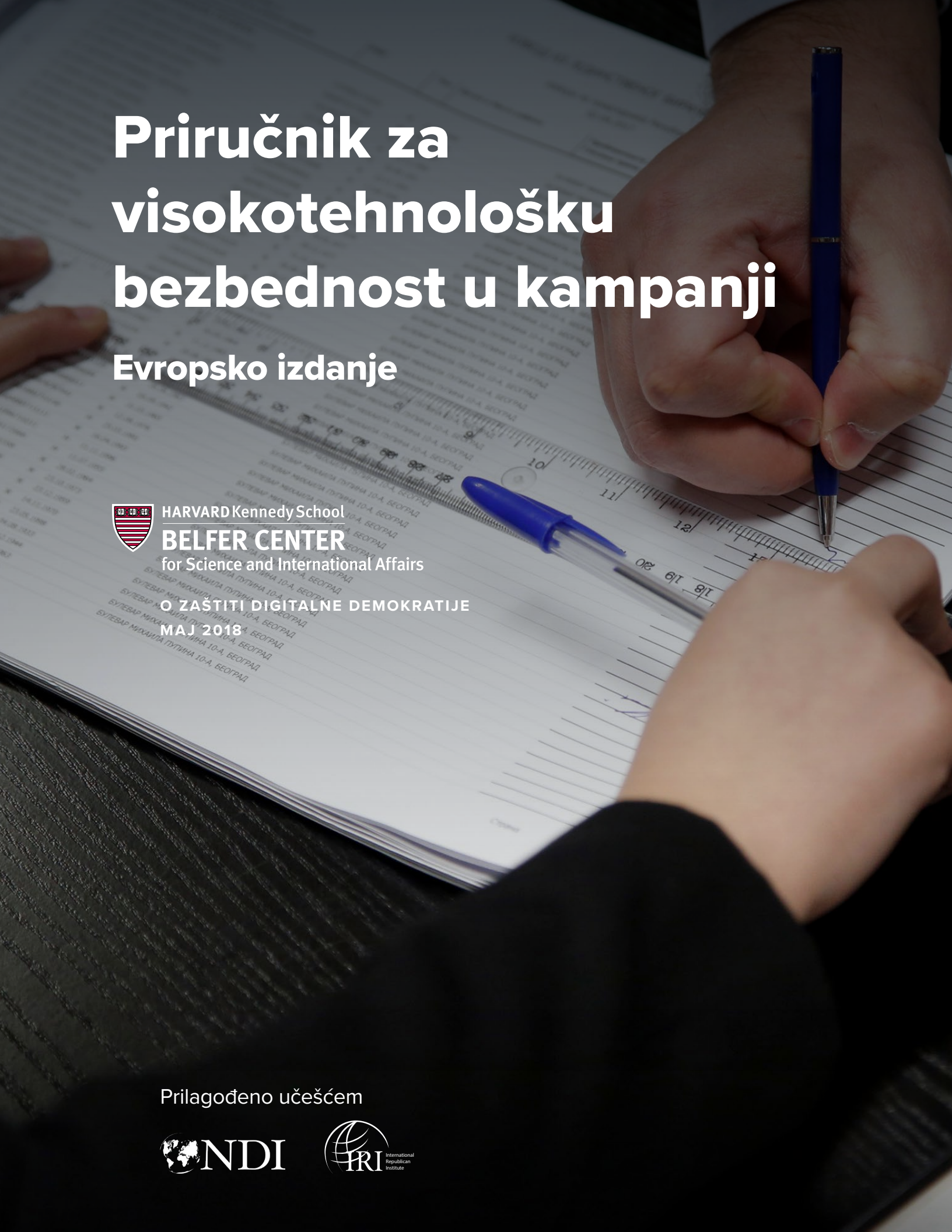

Priručnik za visokotehnološku bezbednost u kampanji

Evropsko izdanje

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

O ZAŠTITI DIGITALNE DEMOKRATIJE

MAJ 2018

Prilagođeno učešćem

NDI IRI International Republican Institute

Defending Digital Democracy Project
Projekat "O zaštiti digitalne demokratije"
Belfer Center za nauku i međunarodne odnose
John F. Kennedy School of Government

79 JFK Street
Cambridge, MA 02138
www.belfercenter.org/D3P

Partneri evropske verzije:

Nacionalni Demokratski Institut
www.ndi.org

Međunarodni Republički Institut
www.iri.org

Dizajn i izgled - Andrew Facini

Fotografija na naslovnici: Srpski premijer i predsjednički kandidat Aleksandar Vučić potpisali su dokument na biračkom mjestu u Beogradu, u nedjelju, 2. aprila 2017. (AP Photo/Darko Vojinović)

Last updated 2018-11-28

Priručnik za visokotehnološku bezbednost u kampanji

Evropsko izdanje

Sadržaj

Dobrodošli

Ljudi se priključuju predizbornim kampanjama iz različitih razloga: da bi se izabrao lider u koga veruju, radi promovisanja određene agende, da bi se pročistile strukture vlasti ili da bi se doživelo adrenalinsko uzbuđenje tokom kampanje. To su neki od razloga zbog kojih se bavimo politikom. Svakako nismo ušli u politiku da bi postali informatički stručnjaci, a pretpostavljamo da niste ni vi.

Nažalost, bezbednosne pretnje se umnožavaju i imaju potencijal da u potpunosti poremete vašu kampanju. Mi smo iz sveta političkih kampanja, podržavamo međunarodne demokratske procese, i imamo saznanja iz prve ruke o načinima na koje hakerski napadi, dezinformacije i rušenje veb sajtova mogu uticati na tok izbora—i smer u kome će se zemlja zaputiti.

D3P čini nezavisan tim eksperata za visokotehnološku bezbednost i politiku iz javnog i privatnog sektora, kao i eksperti s bogatim iskustvom iz političkih kampanja. Ušli smo u partnerstvo sa Međunarodnim republikanskim institutom (IRI) i Nacionalnim demokratskim institutom (NDI) da bismo bolje razumeli međunarodno izborno okruženje kao i da bismo videli kako razmišljati o zaštiti i kako se zaštititi od digitalnih rizika.

Mi smo u različitim političkim strankama i nema puno toga o čemu se slažemo u pogledu javnih politika, ali nas jedna stvar ujedinjuje, a to je verovanje da glasači treba da odluče o ishodu izbora i niko drugi. Naš način života i rada koji se sve više digitalizuju otvara nove mogućnosti za naše protivnike da vrše uticaj na naše političke kampanje i izbore. Mada ne morate biti informatički ekspert da biste vodili uspešnu kampanju, ipak imate odgovornost da zaštitite svog kandidata i organizaciju od protivnika u digitalnom prostoru. Odbrana digitalne demokratije (Defending Digital Democracy), projekat Belfer centra za nauku i međunarodne poslove, izradila je ovaj Priručnik za visokotehnološku bezbednost u kampanji [PDF]. Nacionalni demokratski institut, Međunarodni republikanski institut i na desetine izabranih zvaničnika, stručnjaka za bezbednost i profesionalaca iz političkih kampanja radili su zajedno sa projektom Odbrana digitalne demokratije na prilagođavanju ovog priručnika širem međunarodnom kontekstu.

Informacije prikupljene u ovom priručniku mogu poslužiti svakoj političkoj kampanji bilo koje političke stranke. Osmišljen je da vam pruži jednostavne, primenjive informacije koje će podatke u vašoj kampanji učiniti bezbednijim u odnosu na protivnike koji pokušavaju da napadnu vašu

organizaciju—i demokratiju u vašoj zemlji. Prevashodno se nadamo da će vam ovaj resurs omogućiti da utrošite više vremena na ono zbog čega ste se angažovali—vođenje političke kampanje.

Srećno!

Robby Mook
Menadžer kampanje Hilari Klinton 2016.

Matt Rhoades
Menadžer kampanje Mita Romnija 2012.

P.S. — Da li mislite da se ovaj priručnik može učiniti boljim? Ima li novih tehnologija ili ranjivosti kojima bi trebalo da se pozabavimo? Želimo povratnu informaciju od vas. Molimo vas podelite s nama vaše ideje, priče i komentare na Twitter-u @d3p koristeći heštag #CyberPlaybook ili nam pošaljite poruku elektronske pošte na connect@d3p.org da bismo nastavili da unapređujemo ovaj resurs kako se digitalno okruženje menja.

Autori i saradnici

Ovaj projekat omogućio je desetine ljudi koji su se velikodušno volontirali.

Posebno se zahvaljujemo **Debora Plunkett**-u za vođenje projekta i **Harrison Monsky** za pisanje dokumenta.

Takođe smo zaduženi za ljude koji su navedeni ispod, koji su uložili bezbroj sati u pregledanje nacrta i obezbeđivanje unosa.

DEFENDING DIGITAL DEMOCRACY LEADERSHIP

Eric Rosenbach, Co-Director, Belfer Center

Robby Mook, Belfer Center Fellow

Matt Rhoades, Belfer Center Fellow

AUTHORS AND CONTRIBUTORS

Heather Adkins, Director, Information Security and Privacy, Google

Dmitri Alperovitch, Co-founder and CTO, CrowdStrike

Ryan Borkenhagen, IT Director, Democratic Senatorial Campaign Committee

Josh Burek, Director of Global Communications and Strategy, Belfer Center

Michael Chenderlin, Chief Digital Officer, Definers Public Affairs

Robert Cohen, Cyber Threat Analyst, K2 Intelligence

Chris Collins, Co-Founder, First Atlantic Capital

Caitlin Conley, D3P, Harvard Kennedy School

Julia Cotrone, Special Assistant, Definers Public Affairs

Jordan D'Amato, D3P, Harvard Kennedy School

Mari Dugas, Project Coordinator, D3P, Harvard Kennedy School

Josh Feinblum, D3P, Massachusetts Institute of Technology

John Flynn, Chief Information Security Officer, Uber

Siobhan Gorman, Director, Brunswick Group

Daniel Griggs, Founder and CEO, cmdSecurity Inc.

Stuart Holliday, CEO, Meridian International Center

Eben Kaplan, Principal Consultant, CrowdStrike

Greg Kesner, Principal, GDK Consulting

Kent Lucken, Managing Director, Citibank

Katherine Mansted, D3P, Harvard Kennedy School

Ryan McGeehan, Member, R10N Security

Jude Meche, Chief Technology Officer, Democratic Senatorial Campaign Committee

Nicco Mele, Director, Shorenstein Center

Eric Metzger, Founding Partner and Managing Director, cmdSecurity Inc.

Zac Moffatt, CEO, Targeted Victory

Harrison Monsky, D3P, Harvard Law School

Debora Plunkett, Former Director of Information Assurance, National Security Agency

Colin Reed, Senior Vice President, Definers Public Affairs

Jim Routh, Chief Security Officer, Aetna

Suzanne E. Spaulding, Senior Adviser for Homeland Security, Center for Strategic and International Studies

Matthew Spector, D3P, Harvard Kennedy School

Irene Solaiman, D3P, Harvard Kennedy School

Jeff Stambolsky, Security Response Analyst, CrowdStrike

Alex Stamos, Chief Security Officer, Facebook

Phil Venables, Partner and Chief Operational Risk Officer, Goldman Sachs

Frank White, Independent Communications Consultant

Sally White, D3P, Harvard University

Rob Witoff, Senior Security Manager, Google

Contributors from the **National Democratic Institute** and the **International Republican Institute**

BELFER CENTER WEB & DESIGN TEAM

Andrew Facini, Publications and Design Coordinator, Belfer Center

Pristup u priručniku

Ovaj međunarodni Priručnik za visokotehnološku bezbednost u kampanji je napisao nezavisan međunarodni tim stručnjaka u oblasti visokotehnološke bezbednosti, politike i prava kako bi se predočili jednostavni načini na osnovu kojih se može preduzeti akcija radi suprotstavljanja narastajućim visokotehnološkim pretnjama.

Protivnici u digitalnom prostoru ne biraju mete. Kampanje na svim nivoima—ne samo velike nacionalne političke kampanje—doživele su hakerske napade. Treba pretpostaviti da ste i vi meta. Mada su preporuke iz ovog priručnika opšte primenjive, prevashodno su namenjene kampanjama koje nemaju resursa da angažuju profesionalno osoblje za visokotehnološku bezbednost. Nudimo osnovne gradivne elemente strategije za ublažavanje visokotehnološkog bezbednosnog rizika koju osobe bez tehničke obuke mogu realizovati (doduše, uneli smo i neke stvari za koje će biti potrebna pomoć informatičkih profesionalaca).

Ovo su osnovne preporuke, a ne sveobuhvatna uputstva za postizanje najvišeg mogućeg nivoa bezbednosti. Upućujemo poziv svim kampanjama da obezbede profesionalni input od strane proverenih profesionalaca u oblasti informatike i visokotehnološke bezbednosti kad god je to moguće.

Uvod

Kandidati i kampanje se suočavaju sa zastrašujućim nizom izazova. Postoje događaji koje treba organizovati, volonteri koje treba okupiti, javni skupovi kojima treba upravljati, sredstva koja treba prikupiti, glasači koje treba kontaktirati i neprestani upiti koje generiše savremeni medijski ciklus. Svaki član osoblja mora anticipirati neugodna iznenađenja poput gafova ili političkih oglasa, objavljenih u poslednjem trenutku, u kojima vas napadaju. Visokotehnološki napadi, kampanje s ciljem plasiranja pogrešnih informacija i cenzura na internetu sada su se takođe našle na ovom spisku.

Pošto se kampanje sve više digitalizuju, protivnici su otkrili nove mogućnosti da vam se mešaju u posao, da vas podrivaju i potkradaju. Kineski hakeri su se 2008. godine infiltrirali u Obaminu

i Mekejnovu kampanju i ukrali su velike količine podataka. Ugandski društveni medij je 2016. godine oboren tokom izbora. Sajber operativci za koje se veruje da ih finansiraju ruske vlasti, su 2016. godine ukrali i objavili na desetine hiljada poruka elektronske pošte i dokumenata osoblja predizborne kampanje američke Demokratske partije, pothranjujući time podrivajuće dezinformacijske kampanje. Kenijske političke stranke su se 2017. godine suočile sa široko rasprostranjenim dezinformacijskim kampanjama, a Facebook stranica jedne od glavnih srpskih političkih stranaka je oborena.

Posledice visokotehnoloških upada mogu biti značajne. Vesti o samom upadu, uz postepeno curenje ukradenih informacija, mogu izbaciti iz koloseka političku poruku kandidata mesecima. Napadači koji preopterete i učine nedostupnim vaš veb sajt mogu prekinuti komunikacije s vašim pristalicama ili prouzrokovati gubitak donacija u ključnim trenucima. Krađa ličnih donatorskih ili podataka glasača može proizvesti znatne pravne posledice, izložiti pristalice šikaniranju i obeshrabriti donatore da daju priloge za kampanju. Destruktivni napadi na računare osoblja ili kritične servere koji se koriste u kampanji mogu usporiti aktivnosti tokom kampanje danima ili čak nedeljama. Prevladavanje zbrke koja nastaje će preusmeriti dragocene resurse u jeku tesne izborne trke, bilo da se radi o predsedničkim, parlamentarnim ili opštinskim izborima.

U doglednoj budućnosti, visokotehnološke pretnje će i dalje biti realnost naših kampanja. Pošto je u prvim redovima odbrane demokratije, osoblje kampanje mora prepoznati rizike od napada, razviti strategiju za smanjenje rizika koliko god je to moguće, i realizovati strategije uzvraćanja na napade za trenutak kada se dogodi najgore. Mada nijedna kampanja ne može ostvariti savršenu bezbednost, preduzimanje nekoliko koraka može znatno otežati zlonamernim akterima da nanesu štetu. Ironično je to što najsofisticiraniji državni akteri često biraju najmanje sofisticirane metode napada, ostrvljujući se na ljude i organizacije koje zanemare osnovne bezbednosne protokole. To je naš glavni razlog za izradu ove evropske verzije Priručnika za visokotehnološku bezbednost u kampanji.

U današnjim kampanjama, visokotehnološka bezbednost je odgovornost svih. Ljudska greška je redovno uzrok visokotehnoloških napada koji su dobili publicitet u medijima, i na kandidatu je i onima koji vode kampanju da utkaju svest o bezbednosti u kulturu organizacije. Odluke koje donose ljudi jednako su važne kao i softver koji koriste. U budućnosti će najbolje kampanje imati jasne standarde za naporan rad, doslednost poruke, lojalnost prema timu—i praćenje dobrog bezbednosnog protokola.

Pre nego što krenemo s našim preporukama, hajde da začas postavimo okvir problema:

- **okruženje** u kome se vodi vaša kampanja;
- **pretnje** s kojima će se vaša kampanja verovatno suočiti; i
- **značaj** upravljanja rizikom od visokotehnoloških napada.

Ranjivo okruženje kampanje

Današnje kampanje su posebno meke mete. Često su im svojstvene privremenost i prolaznost. Nema se vremena, niti novca za razvoj dugoročnih, temeljno isprobanih bezbednosnih strategija. Veliki broj novih članova osoblja se može angažovati brzo, bez utroška puno vremena za njihovu obuku. Oni mogu donositi sopstvene uređaje od kuće—kao i maliciozni štetni softver koji na njima vreba iz potaje! Mnogi saradnici žive i rade na stotine kilometara daleko od štaba kampanja. Stvari se odvijaju brzo, ulozi su često veliki i ljudi smatraju kako nemaju vremena da da se pozabave visokotehnološkom bezbednošću. Mnogo je mogućnosti da nešto pođe naopako.

Istovremeno, u kampanjama se sve više oslanjamo na privatne informacije o glasačima, donatorima i javnom mnjenju. Takođe se tokom kampanja skladište osetljivi dokumenti poput istraživanja o političkim protivnicima koja se mogu upotrebiti za njihovo diskreditovanje, studije o ranjivosti protivnika, spiskovi pristalica, dokumenti o proveri osoblja, prvi nacrti politika i elektronska pošta. Rizici od potencijalnih napada su sve veći, kao i posledice.

OPASNOST OD NAPADA

Zamislite ovaj scenario... Mesec je dana do izbora, a izborna trka je neizvesna. Stižete u sedište kampanje rano, osvežite se kafom ili čajem, sedate za svoj sto i ulogujete se na svoj računar. Pojavljuje se crn ekran, i potom jeziva karikatura vašeg kandidata, propraćena porukom. Vaši čvrsti diskovi su potpuno obrisani. Svaka digitalna informacija koju ste prikupili—memorandumi, namenske liste, računovodstveni izveštaji—nestali su. Da biste ih povratili, čitate dalje, to će vas koštati ni manje, ni više nego milion—ili će vas koštati odustajanja od bitne političke pozicije.

Neidentifikovana grupa je upala u vaš računar pre više meseci i neprimetno je krala poruke elektronske pošte, strateške memorandume, donatorske adrese i matične brojeve socijalnog osiguranja ili jedinstvene matične brojeve osoblja kampanje. Hakerska grupa je provela sedmice pročešljavajući plen u potrazi za prljavim vešom i distribuirala je najvažnije informacije na društvenim medijima i putem veb sajta, lakog za korišćenje, namenjenog samo distribuiranju najznačajnijih informacija. Posebno je istaknut dugačak „samoistraživački“ izveštaj o vašem kandidatu. Za sada, veb sajt kampanje je nedostupan javnosti, nalozi na društvenim medijima su suspendovani zbog isticanja nepristojnih slika, a nigde na vidiku nema računara koji radi.

Pretnje s kojima se kampanje suočavaju

Na nesreću kampanja i demokratija širom sveta, domaći i strani protivnici mogu pomisliti da nanošenje štete ili pomaganje određenom kandidatu ide u prilog njihovim interesima, bez obzira da li to znači izazivanje haosa ili konfuzije među glasačima, ili kažnjavanje zvaničnika koji je govorio protiv njih. To može zvučati kao fikcija iz trilera, ali realnost je da sofisticirana obaveštajna služba, visokotehnološki kriminalci ili hakeri-aktivisti kivni na kandidata mogu odlučiti da ste meta vi ili neko iz vaše kampanje. To su pretnje za koje rukovodioci i osoblje kampanje moraju shvatiti da su moguće.

Kada dezinformacije i izmanipulisani komunikacijski kanali kampanje postanu izvor prevara i obmana za građane širom sveta, ukradene, izmanipulisane i obelodanjene informacije mogu

izazvati realne posledice po vaše izbore. Mehanizmi koje imate na raspolaganju za zaštitu vaših podataka i održavanje komunikacijskih kanala su značajniji nego ikada ranije.

KO VRŠI HAKERSKE NAPADE?

Kampanje se suočavaju s pretnjama informacijama i visokotehnološkoj bezbednosti za koje je odgovaran širok spektar aktera. Usamljeni neetički hakeri („hakeri s crnim šeširom“) i visokotehnološki kriminalci pokušavaju da kompromituju kampanje radi sticanja lične koristi, ozloglašenosti ili prosto želje da vide šta mogu da učine. Nacionalne države predstavljaju najuporniju i najistrajniju pretnju. Ruske špijunske grupe poznate pod imenom „Fancy Bear“ –(„Pomodni medved“) (APT 28) i „Cozy Bear“ („Ugodni medved“) (APT 29) bile su umešane u hakerske napade na kampanje u Americi 2016, godine. Kinezi su se znatno više usredsredili na prikupljanje podataka. Veruje se da su bili aktivni 2008. i 2012. tokom američkih predsedničkih kampanja, ali nema dokaza da su objavili bilo šta od ukradenih materijala. Ozloglašena je već odmazda Severnokorejanaca prema filmskoj producentskoj kući “Sony Pictures Entertainment” zbog igranog filma Intervju, kada su ukrali i objavili elektronsku poštu firme i oborili njihove sisteme. U nekim zemljama, opozicione kampanje se mogu suočiti s pretnjama od strane sopstvene vlade takođe. Povišene međunarodne tenzije—pogotovo u vezi sa izborima s visokim ulozima—bi mogle podstaći još više napada u budućnosti.

Upravljanje visokotehnološkim rizicima

Rizik se najbolje može razumeti iz tri dela. Prvo, postoje ranjivosti: slabosti u vašoj kampanji koje vaše informacije čine podložnim krađi, izmenama ili uništavanju. Ranjivosti mogu proisteći iz hardvera, softvera, procesa i nivoa budnosti vašeg osoblja. Potom postoje istinske pretnje: nacionalne države, hakeri-aktivisti i druge nedržavne grupe sposobne da eksploatišu te ranjivosti. Rizik postoji tamo gde se ranjivosti i pretnje susreću. Konačno, postoje posledice –efekti koji nastaju kad zlonamerni akteri iskoriste neublažene rizike.

Ne postoji ništa što vi ili vaša kampanja možete učiniti da biste sprečili sâme pretnje—one su posledica širih geopolitičkih, ekonomskih i društvenih sila. Ono što možete učiniti jeste da znatno smanjite verovatnoću uspeha vaših protivnika tako što ćete smanjiti vašu ranjivost. Smanjivanje ranjivosti smanjuje rizik—na vama je da odlučite koje ranjivosti je najvažnije smanjiti. Na primer, možete odlučiti da je najštetnija stvar koju haker može napraviti krađa „samoistraživačkog“ izveštaja vašeg kandidata, pa ćete posvetiti dodatne resurse obezbeđivanju vašeg skladištenja podataka u oblaku (cloud-based storage), postaviti dugačke lozinke i ograničiti pristup na mali broj ljudi. Možete odlučiti da druge dokumente o kampanji učinite šire dostupnim i manje bezbednim pošto je većem broju ljudi potreban pristup da bi obavili svoje poslove, a ne bi naneli veliku štetu ako bi „procureli“. Obratite pažnju da se na korake koji se preduzimaju u kampanjama radi obezbeđivanja sopstvenih podataka i reagovanja na bilo kakve incidente takođe primenjuju isti zakoni o zaštiti podataka i privatnosti koji se usvajaju širom sveta, poput Opšte uredbe o zaštiti podataka (GDPR) u Evropi.

Postoje tehnički aspekti ublažavanja rizika i mi predočavamo mnoge tehničke preporuke u ovom priručniku, ali najvažniji je vaš holistički pristup. U svojstvu lidera predizborne kampanje, najvažnija stvar koju možete uraditi jeste da pravite suštinske odabire, na primer, ko ima pristupa informacijama, koje se informacije čuvaju ili odbacuju, koliko vremena posvećujete obuci, i vaše sopstveno ponašanje kao primera za uzor. Pošto ste profesionalac u kampanji, upravljanje rizikom je vaša kako tehnička, tako i ljudska odgovornost. Na vama je da odlučite koji su podaci i sistemi najvredniji i za koje resurse ćete se opredeliti da ih zaštitite.

Obezbeđivanje vaše kampanje

Naše bezbednosne preporuke se temelje na tri principa:

1. Priprema:

Uspeh skoro svake preporuke iz priručnika zavisi od toga da li rukovodstvo kampanje stvara kulturu budnosti u smislu bezbednosti koja minimizuje slabosti. To znači uspostavljanje jasnih osnovnih pravila koja se primenjuju odozgo nadole i prihvaćena su odozdo nagore.

2. Zaštita:

Zaštita je od kritične važnosti. Kada otkrijete da imate bezbednosni problem, već je isuviše kasno. Izgradnja najsnažnijih odbrana koje vam vreme i novac dozvoljavaju je ključno za smanjenje rizika. Internet i bezbednost podataka najbolje funkcionišu u slojevima: ne postoji jedinstvena, neprobojna tehnologija ili proizvod. Kombinacija nekoliko osnovnih mera mogu učiniti digitalnu arhitekturu kampanje neprobojnijom za upad i otpornijom ukoliko se ugrozi, uštedevši vam na kraju u kampanji vreme i novac u budućnosti.

3. Istrajnost:

Kampanje se sada suočavaju s protivnicima koji raspolažu sa sve većim nivoom resursa i ekspertize; čak ni najbudnija kultura i najžilavija infrastruktura možda neće moći da spreče narušavanje bezbednosti. Kampanje treba da izrade unapred plan za reagovanje na narušavanje bezbednosti u slučaju da do toga dođe.

Neke kampanje imaju više vremena i novca za visokotehnološku bezbednost od drugih. Zato naše preporuke nude dva nivoa bezbednosti: „**dobar**“ i „**unapređen**“.

„Dobar“ nivo predstavlja sve što se u kampanji mora učiniti da bi se imao minimalan nivo bezbednosti. Uvek bi trebalo težiti da se uradi što više koliko to vreme, novac i ljudi dozvoljavaju, zbog čega preporučujemo korišćenje „unapređenog“ nivoa bezbednosti kad god je to moguće. Ukoliko imate resurse za pribavljanje obučene informatičke podrške na dobrom glasu, to je dobro utrošen novac. Pretnje neprestano evoluiraju i profesionalne informatičke usluge će vam pomoći da odete dalje od onoga što vam ovaj priručnik pruža i da budete korak ispred najnovijih pretnji sa rešenjima za svoju situaciju.

Upravljanje

Menadžeri kampanje treba da preuzmu odgovornost za svoju strategiju visokotehnološke bezbednosti, ali većina će delegirati njen razvoj i nadzor zameniku ili direktoru operacija. Važno je da visokotehnološka bezbednost bude tesno integrisana u rad na ljudskim resursima i informatičkoj tehnologiji pošto će ispravno uvođenje osoblja u posao, nabavka opreme i kontrola sistema dozvola biti od kritičnog značaja za vašu strategiju. Mnoge male kampanje će se oslanjati na podršku volontera u informatičkoj tehnologiji i visokotehnološkoj bezbednosti. Možete upotrebiti ovaj priručnik kao vodič za vašu diskusiju s vašom volonterskom podrškom. Ključno je temeljno proveriti volontere koji vas podržavaju i brižljivo kontrolisati pristup kako vam volonterska podrška ne bi stvarala nove ranjivosti. Trebalo bi da se postarate da član osoblja iz kampanje nadzire rad na informatičkim tehnologijama i kontroliše dozvole za pristup različitim sistemima.

Kada početi

Kakav god da model podrške imate, s *visokotehnološkom bezbednošću bi trebalo krenuti od Prvog Dana*. Dalje sledi „lista za proveru pet najvažnijih mera" koje su od apsolutno vitalnog značaja. Postarajte se da budu spremne od samog početka, čak i ako imate samo jednog ili dva člana osoblja, a potom primenite ostale „dobre" preporuke čim pre to možete. Ako ove mere nisu bile deo vašeg prvog digitalnog plana, ne brinite. Nije isuviše kasno da usvojite delotvorne bezbednosne mere i zaštitite ono što već radite.

Trošak

Puno toga što preporučujemo ovde je besplatno ili košta malo. Zapravo, sve na našoj listi pet najvažnijih mera je besplatno, osim pribavljanja platforme zasnovane na oblaku, što će vas koštati samo nekoliko dolara mesečno po zaposlenom. Velike kampanje treba da odvoje dovoljno resursa iz budžeta za hardver i softver radi sprovođenja odgovorne strategije, ali to bi trebalo da bude veoma mali procenat višemilionskog budžeta kampanje u dolarima. Manje kampanje će biti u mogućnosti da primene preporuke odavde za nekoliko stotina do nekoliko hiljada dolara zavisno od toga koliko osoblja ili volontera radi na kampanji.

Bilo kakav pomen prodavaca opreme i usluga ima za cilj da se pruže primeri uobičajenih rešenja, ali ne predstavljaju komercijalne preporuke. Ako se pojave izazovi pri implementaciji proizvoda ili usluga, podstičemo vas da se neposredno obratite dobavljačima opreme, koji vam obično mogu pružiti tehničku pomoć na nivou korisnika. U pogledu izbora proizvoda i usluga, podstičemo svaku kampanju da se konsultuje sa stručnjacima za visokotehnološku bezbednost ili da sprovede nezavisno istraživanje kako bi se pronašao najbolji proizvod za sopstvene potrebe.

Lista za proveru pet najvažnijih mera

1. Uspostavite svest o kulturi informatičke bezbednosti:

Shvatite ozbiljno visokotehnološku bezbednost. Preuzmite odgovornost za smanjenje rizika, obučite osoblje i volontere, i dajte primer. Ljudska greška je najčešći uzrok narušavanja bezbednosti.

2. Koristite oblak:

Velika komercijalna usluga skladištenja podataka u oblaku će biti znatno bezbednija od bilo čega što možete sâmi postaviti s ograničenim resursima. Razmotrite korišćenje kancelarijskog programskog paketa u oblaku poput GSuite ili Microsoft365 koji će vam obezbediti sve vaše osnovne kancelarijske funkcije i bezbedan prostor za skladištenje informacija (vidi „Šta je oblak?“ na str. 21).

3. Koristite verifikaciju u 2 koraka (2FA) i jake lozinke:

Postavite verifikaciju u 2 koraka (2FA) da biste imali dodatni nivo zaštite za sve važne naloge, uključujući vaš kancelarijski paket programa, bilo koje druge usluge elektronske pošte ili skladištenja podataka, i vaše naloge na društvenim medijima. Koristite mobilnu aplikaciju ili fizički ključ za vaš drugi stepen autorizacije, a ne SMS poruku. Za vaše lozinke kreirajte NEŠTOZAISTADUGAČKOPOPUTOVOGNIZA, a ne nešto zaista kratko poput Th1$. Nasuprot široko rasprostranjenom verovanju, dugačak niz nasumičnih reči je teže dešifrovati nego nešto kratko s Pun0 $ymB01a. Nikada ne ponavljajte lozinke; program za upravljanje lozinkama vam takođe može pomoći tako što će vam dopustiti da kreirate nasumične jake lozinke i proverite postojeće lozinke kako biste identifikovali one koje su već korišćene.

4. Koristite šifrovane poruke za osetljive razgovore i materijale:

Korišćenje alatke za poruke sa enkripcijom na mobilnim telefonima, poput aplikacija Signal ili Wickr, za osetljive poruke i dokumente znači da vaši protivnici ne mogu doći do njih ako budu upali u vašu elektronsku poštu. Enkripcijom se šifruju podaci čime se dramatično smanjuje verovatnoća da bi neko mogao da pročita vaše poruke, čak i ako presretne vaše podatke.

5. Planirajte i pripremite se:

Imajte plan u slučaju da se ugrozi vaša bezbednost. Znajte koga da pozovete za tehničku pomoć, budite upoznati s vašim pravnim obavezama i budite spremni da prenesete vest o tome unutar i izvan kampanje što je brže i delotvornije to moguće.

Koraci za obezbeđivanje vaše kampanje

Korak 1: Ljudski faktor

Visokotehnološka bezbednost je u suštini ljudski, a ne tehnički problem. Najbolja tehnička rešenja na svetu neće imati efekta ako se ne primenjuju valjano, ili ako se neprestano ne ažuriraju kako tehnologija napreduje. Uspešne prakse u oblasti visokotehnološke bezbednosti zavisi od uspostavljanja kulture bezbednosti.

DOBAR NIVO BEZBEDNOSTI — Šta treba da uradite

1. Uspostavite snažnu kulturu informatičke bezbednosti koja potcrtava bezbednost kao standard za pobedničku kampanju. Baš kao što se osoblje kampanje upućuje da ne krši propise o finansiranju kampanja, zaposleni bi takođe trebalo da znaju da treba izbegavati klikove na linkove ili otvaranje priloga u porukama elektronske pošte od nepoznatih pošiljalaca.

    a. **Uvođenje u posao**: Obezbedite osnovnu obuku iz informatičke bezbednosti kada uvodite novo osoblje u posao. Možete podeliti osoblju štampana uputstva tokom obuke.

    b. **Obuke**: Učinite bezbednost delom vaših tekućih obuka za osoblje, poput događaja za rukovodeće osoblje ili predizborne obuke za povećanje izlaznosti na izborima. Obezbedite dodatnu obuku za one koji imaju osetljive uloge, poput kandidata, osoblje za odnose s medijima, rukovodeće osoblje i svakog s ovlašćenjima sistemskog administratora na mreži. Rukovodioci bi trebalo da traže da bezbednosna podešavanja najvažnijih osoba u kampanji—uključujući kandidata—proveri lice zaduženo za informatičke tehnologije (to može biti sâm rukovodilac). Nemojte se ustezati ili se mlako odnositi prema bezbednosti za kandidata i ostale veoma važne osobe!

    c. **Dajte primer**: Rukovodeće osoblje u kampanji i kandidat moraju imati vidljivo vodeću ulogu, zagovarajući visokotehnološku bezbednost tokom obuka. Rukovodeće osoblje bi trebalo da periodično naglašava značaj visokotehnološke bezbednosti pred mlađim članovima osoblja na sastancima i u telefonskim razgovorima. Ne dopustite da samo tehnički eksperti vode obuke. Rukovodilac kampanje ili direktor operacija može biti uticajniji prenosilac poruke upravo zato što ih osoblje vidi kao manje „tehničke“ osobe.

2. Sprovedite temeljnu proveru osoblja, volontera i pripravnika—svakoga kome je potreban pristup informacijama u kampanji—da biste izbegli davanje ovlašćenja nekome ko želi da ukrade podatke ili sabotira vaše sisteme.

a. Utvrdite definiciju osetljivih informacija i pravila za njihovo korišćenje. Na primer, možete odlučiti da klasifikujete sve ankete, istraživačke materijale, strateške memorandume i s tim povezanu elektronsku poštu kao „osetljive“.

b. Zabranite prenos osetljivih informacija preko komunikacionih kanala kojima ne upravlja i koje ne obezbeđuje vaša kampanja. Možete tražiti da se osetljive informacije prenose samo putem poruka zaštićenih enkripcijom (vidi Korak 2).

3. Potvrdite da konsultanti i dobavljači s pristupom osetljivim informacijama imaju bezbednu elektronsku poštu i skladištenje podataka (vidi Korak 2). Ako niste sigurni, tražite od dobavljača i konsultanata da koriste nalog u vašem kancelarijskom paketu programa u oblaku (vidi Korak 2).

4. Kontrolišite pristup važnim internet uslugama, poput zvaničnih naloga kampanje na društvenim medijima, da biste sprečili pristup od strane neovlašćenih pojedinaca. Postarajte se da oni koji napuste kampanju nemaju više pristupa nalozima povezanim s kampanjom. To lako možete uraditi koristeći alatku za upravljanje nalogom na društvenim medijima koja funkcioniše kao mrežni prolaz za sve vaše naloge. Ako neko napusti kampanju, trebalo bi da odmah ugasite njihov nalog.

5. Edukujte članove osoblja o pretnji koju predstavlja „pecanje“ (phishing). Postarajte se da znaju kako da prepoznaju i izbegnu sumnjive linkove i naglasite značaj identifikovanja i izveštavanja o potencijalnim napadima korišćenjem „pecanja“. U okviru robusne kulture bezbednosti u kampanji, rukovodeće osoblje bi trebalo da prepozna i pohvali svakoga ko izvesti o sumnjivom ponašanju u njihovom sistemu ili prizna da je kliknuo na potencijalno maliciozan link.

6. Upoznajte se sa svojim pravnim okruženjem. Na nekim mestima, uključujući Evropsku uniju, standardi zaštite privatnosti nameću posebne uslove za sve podatke koje prikupite u sklopu kampanje, pogotovo informacije putem kojih se mogu lično identifikovati osobe kao što su to demografski podaci ili adrese.

Štampana uputstva

» Za članove osoblja
» Za članove porodice

UNAPREĐEN NIVO BEZBEDNOSTI — Preduzmite sledeći korak

1. Softverski proizvodi poput Phishme i KnowBe4 mogu pomoći u obuci vašeg osoblja slanjem lažnih „pecaroških“ poruka elektronske pošte. To je bezbedan, brz i delotvoran način da se nauči ko je sklon da klikne na ponuđeni link tako da ih možete dodatno obučiti. Mnogi među ovim proizvodima takođe filtriraju neke „pecaroške“ napade iz vašeg elektronskog poštanskog sandučeta.

2. Ako imate resursa, unajmite profesionalca za informatičke tehnologije koji bi vodio sisteme vaše kampanje i stručnjaka za informatičku bezbednost koji bi pomogao da se zaštiti, održava i prati digitalna infrastruktura kampanje. On ili ona može organizovati redovnu obuku iz bezbednosti i testirati vaše osoblje i sisteme, prilagođavajući bezbednosna rešenja vašim potrebama.

3. Zaključite ugovor sa firmom za visokotehnološku bezbednost koja bi dala bezbednosna rešenja, pregledala vaše sisteme odbrane i/ili pratila vaše sisteme zbog mogućeg upada. Znajte koju firmu da kontaktirate ako dođe do upada u sistem i ako vam je potrebna hitna podrška za reagovanje na incident. To je alternativa unajmljivanju stručnjaka za informatičku bezbednost s punim radnim vremenom. Istražite i izaberite firmu s dobrom reputacijom—ne pružaju sve firme za visokotehnološku bezbednost isti nivo usluge.

RAD SA PROFESIONALCIMA U OBLASTI BEZBEDNOSTI

Ako se odlučite da radite sa profesionalcima za bezbednost, kako ćete proceniti koja je prava osoba ili firma za vas? Bilo da to činite pomoću ličnih preporuka ili javnih pozitivnih recenzija, važno je izbeći skupu, a nedelotvornu podršku. Kada razgovarate s potencijalnim profesionalcima za bezbednost, pitajte ih kako su reagovali na ranije bezbednosne incidente i kako su osposobili druge da rade u bezbednijem okruženju. Vaši nacionalni stranački odbori ili profesionalci od poverenja u kampanji vam možda mogu preporučiti opcije za odabir. Imajte na umu da kultura utiče na bezbednost, te da čak ni najbolje preporuke ne moraju nužno dovesti do rezultata ukoliko se preporuke ne slede (npr. puko angažovanje firme za bezbednost neće rešiti vaše probleme).

Korak 2: Komunikacija

Nisu sve metode komunikacije jednako bezbedne, stoga budite promišljeni u pogledu toga kako komunicirate. Rukovodstvo kampanje bi trebalo da postavi standard kojim se podstiču razgovori licem u lice kad god je to moguće, a obeshrabruju nepotrebne ili suvišne poruke elektronske pošte. Sve što napišete u poruci elektronske pošte se može objaviti u novinama ili na društvenim medijima—možda nakon zlonamernih prepravki. Bez obzira da li se radi o telefonskim pozivima, slanju tekstualnih poruka ili elektronske pošte, različiti proizvodi i usluge nude različite nivoe zaštite tako da treba obaviti istraživanje pre nego što odlučite koje će sisteme vaša kampanja koristiti.

DOBAR NIVO BEZBEDNOSTI — Šta treba da uradite

1. Koristite najbezbednije moguće sisteme za komunikaciju.
    a. Koristite servise za poruke sa enkripcijom s kraja na kraj komunikacionog kanala poput Signal-a ili Wickr-a, pogotovo za tekstualne poruke, deljenje dokumenata i telefonske pozive. U mnogim kampanjama se zahteva da se osetljive informacije prenose jedino putem servisa za poruke s enkripcijom. Najčešće je najlakše za osoblje kampanje da usvoji naviku korišćenja ovih aplikacija za celokupnu rutinsku komunikaciju (to je pogotovo pametno učiniti u slučaju pojedinaca koji su izloženi visokom riziku poput kandidata). Signal i Wickr objavljuju svoj izvorni programski kôd radi analize i pružaju funkcionalnost koja smanjuje rizik poput omogućavanja automatskog brisanja poruka. Postarajte se da se vaše poruke ne sinhronizuju s vašim računarom ili nalozima u oblaku bez enkripcije.
    b. Isključite opciju arhiviranja za servise za poruke, poput Google Chat-a i Slack-a, tako da se stare prepiske ne mogu ukrasti kasnije. To iziskuje da otvorite „podešavanja“ i podesite vremenske periode za „politiku čuvanja poruka“. Kod nekih servisa to morate uraditi za svaku pojedinačnu razmenu poruka. Preporučujemo da čuvate poruke iz razgovora jednu sedmicu ili kraće.
2. Koristite kancelarijski programski paket u oblaku koji omogućava bezbednu komunikaciju putem elektronske pošte, kreiranje dokumenata, ćaskanja i deljenja datoteka, kao što su to GSuite ili Microsoft365. Na primer, GSuite obuhvata Google Drive za deljenje datoteka, Gmail za hosting usluga, Google Hangouts za ćaskanje i Google Docs za rad u procesoru teksta, tabelama i prezentacijama. Microsoft365 nudi OneDrive/SharePoint za deljenje datoteka, Outlook/Exchange za elektronsku poštu, Microsoft Teams za ćaskanje i Microsoft Office za rad u procesoru teksta, tabelama i prezentacijama. Osim ukoliko ne angažujete veoma iskusne (i potencijalno skupe) profesionalce za bezbednost, sistemi u oblaku kojima upravljaju velike kompanije biće bolje zaštićene nego bilo koji serveri koje biste vi mogli da postavite za potrebe vaše kampanje. Postoje besplatne verzije oba proizvoda, ali plaćene verzije vam pružaju znatno veće mogućnosti administriranja. Google takođe nudi besplatne servise za zaštitu organizacija u okruženju ispunjenom pretnjama kao što su

Outline, sopstvena virtualna privatna mreža (VPN); Project Shield, servis za zaštitu vašeg veb sajta od napada koji bi ga onesposobio; i Password Alert, koji vas upozorava ako upišete vašu lozinku za Gmail na „pecaroškom“ sajtu.

3. Izbrišite vašu elektronsku poštu

    a. Uključite opciju za automatsko brisanje stare pošte u vašoj aplikaciji za elektronsku poštu kako biste smanjili broj poruka elektronske pošte koje bi eventualno mogle biti ukradene. To obično iziskuje otvaranje „podešavanja“ i izmenu „politike čuvanja poruka“ tako što aktivirate kraći period za čuvanje poruka. Kako biste se postarali da se poruke elektronske pošte ne zadržavaju u fascikli „obrisane stavke“, prilagodite podešavanja da bi se fascikla „obrisane stavke“ automatski praznila posle izvesnog perioda. Preporučujemo da poruke elektronske pošte čuvate jedan mesec ili kraće, osim ukoliko ne postoji zakonska obaveza čuvanja poruka tokom dužeg vremena. Ono što nemate vam ne mogu ukrasti.

4. Bezbedni lični nalozi

    a. Ne bi trebalo da se poslovi vezani za kampanju ikada obavljaju preko ličnih naloga, no protivnici će svakako pokušati da hakuju lične naloge tako da vaše osoblje treba da koristi jake lozinke i verifikaciju u 2 koraka za svoje lične naloge takođe (to je sadržano u našem štampanom materijalu za podelu osoblju).

ŠTA JE OBLAK?

„Usluge oblaka“ omogućavaju upravljanje i pristup informacijama uskladištenim daljinski na internetu. Takve usluge se pružaju na serverima izvan vaše lokacije, a njima upravljaju treće strane—kompanije; one obuhvataju mnoge uobičajene usluge koje možda već koristite poput Gmail-a ili Dropbox-a. Dobro je skladištiti informacije kod pružaoca usluga u oblaku od poverenja umesto na vašem ličnom računaru jer ovi pružaoci usluga u oblaku imaju sredstava, tehničkih resursa i stručno znanje koji njihove servere čine bezbednijim od čvrstog diska vašeg laptopa ili kancelarijskog servera. Takođe imaju puno tehničkog osoblja koje radi na odbrani od sofisticiranih napada na njihove mreže (i, stoga, na odbrani vaših podataka takođe). To je poput razlike između čuvanja ušteđene gotovine ispod dušeka i deponovanja u bezbednom sefu banke. Korišćenje usluga u oblaku nudi dodatnu zaštitu od gubitka podataka ako se neki uređaj izgubi ili dođe do hakerskog upada. Skladištenje podataka u oblaku se nudi u sklopu sveobuhvatnih paketa kancelarijskih bezbednosnih usluga poput GSuite-a i Microsoft365. Drugi pružaoci takvih usluga su i Dropbox ili Box. Važno je imati na umu da se od ovih međunarodnih korporacija mogu zahtevati istorijski podaci o kontaktima, elektronskoj pošti ili sadržajima datoteka. Većina velikih korporacija, uključujući sve koje su pomenute u ovom dokumentu, imaju stroge politike u pogledu toga kada će se povinovati takvim zahtevima.

ŠTA AKO NEMAM POVERENJA U OBLAK?

Neke organizacije uznemirava ideja da svoje informacije povere trećoj strani—firmi. Ako insistirate na upravljanju sopstvenom tehnološkom infrastrukturom, budite svesni toga da ćete možda morati da se branite od napada bezbednosnih snaga nacionalnih država. Evo šta treba razmotriti:

- Imaćete odgovornost da razumete, obezbedite i „zakrpite“ sve aspekte svojih sistema, uključujući operativne sisteme, serverske aplikacije, sâm softver, baze podataka i tehnologije za uspostavljanje veza.
- Moraćete se postarati da veza sa vašim ključnim platformama bude veoma pouzdana, a nikako ranjiva na manipulaciju, cenzuru ili napad metodom „distribuiranog uskraćivanja usluge“ (DDOS, Distributed Denial of Service, pokušaj napadača da računar(e) učini nedostupnim korisnicima kojima je namenjen).
- Biće potrebno da aktivno pratite situaciju zbog mogućih hakerskih napada i da imate nekoga na dežurstvu 24 sata dnevno, 7 dana u nedelji.
- Biće potrebno da upravljate bezbednim rezervnim kopijama podataka uskladištenim izvan vaših prostorija.
- Ukoliko vam preti rizik od fizičkog napada, vaše informacije bi mogle biti zaplenjene.

ŠTA JE ENKRIPCIJA?

Enkripcija je način šifrovanja informacija kada se one prenose između korisnika ili kada su uskladištene tako da ih niko ne može rastumačiti osim nameravanog primaoca. Zamislite to na ovaj način: korisnik „šifruje“ podatke kad ih pošalje i samo nameravani primalac poseduje ključ za dešifrovanje. Mudro je koristiti enkripciju, pogotovo za osetljive informacije pošto čak i ako protivnik ukrade vaše podatke, malo je verovatno da će biti u stanju da ih iščita. Većina aplikacija koje koriste enkripciju, kao što su to Signal ili Wickr, omogućavaju da se taj proces odvija glatko. Enkripcija s kraja na kraj komunikacionog kanala je značajna odlika programa za komunikaciju. To znači da se vaša poruka čuva u tajnosti počev od vašeg mobilnog telefona ili računara sve do njene destinacije, a niko, uključujući samu firmu koja je izradila aplikaciju, ne može pročitati poruke. Ako je to moguće, primenite enkripciju na celom čvrstom disku takođe; ako ga ukradu ili ga zaboravite u autobusu, niko neće moći da iščita njegov sadržaj.

CENZURA, PRISMOTRA I GAŠENJE INTERNETA

Nažalost, u mnogim delovima sveta su sve izraženiji trendovi zauzdavanja interneta kao jednog otvorenog, demokratskog prostora. To može podrazumevati blokiranje kritičnih komunikacionih kanala kao što su, na primer, WhatsApp ili Twitter; cenzurisanje vaših javnih veb sajtova; ili agresivno špijuniranje građana koji posećuju vaše internet lokacije i onoga što vaše osoblje radi na internetu. U najgorim situacijama, koje su zabrinjavajuće učestale, neka zemlja može u potpunosti onemogućiti pristup internetu.

Uvek imajte rezervni plan. Ako je vaša stranka ili kampanja posebno zavisna od veb sajta vaše predizborne kampanje, pobrinite se da vaša stranica na Fejsbuku sadrži najvažnije informacije u slučaju da je vaš veb sajt blokiran ili cenzurisan. Ako je WhatsApp osnovni komunikacioni kanal, budite spremni da koristite SMS poruke ili da imate rezervnu kopiju telefonske liste s brojevima svih osoba. Ako praćenje internet saobraćaja ili aktivnosti na internetu vašeg osoblja u kampanji može prouzrokovati nevolje, razmotrite korišćenje alatki za zaobilaženje toga ili anonimizaciju kao što su Tor Browser[1], Psiphon[2] ili Outline[3] uradi-sam VPN. Imajte svoju listu novinara pri ruci i u slučaju značajnijih promena u pogledu cenzure ili gašenja interneta, pomozite im da od toga naprave priču.

[1] https://www.torproject.org/projects/torbrowser.html.en
[2] https://www.psiphon3.com/en/index.html
[3] https://getoutline.org/en/home

KAKO ODRŽATI VAŠE VEB SAJTOVE NA INTERNETU

Veb sajt vaše kampanje verovatno je jedna od vaših najvažnijih javnih komunikacijskih platformi i jedan je od najlakših načina da vas građani pronađu. To čini vaše prisustvo na internetu pogotovo primamljivom metom za maliciozne hakere ili beskrupulozne rivale. Razmotrite korišćenje neke uređene platforme za hosting kao što su to Wordpress.com, Wix ili Google Pages gde nemate odgovornost administratora za bezbednost na vašem veb sajtu. Ako želite da upravljate sopstvenim veb sajtom, budite sigurni da ste upravo vi sâmi ekspert ili da ste u mogućnosti da angažujete profesionalce kako bi se sačuvali od hakera.

Sve češće napadači pribegavaju „distribuiranom uskraćivanju usluge“ (DDOS) da bi oborili vaš veb sajt tokom kritičnih perioda putem slanja ogromnog broja lažnih upita. Mreže za distribuciju sadržaja (Content Distribution Networks - CDNs) su u mogućnosti da sačuvaju „keširanu“ kopiju vašeg sajta na moćnim serverima širom sveta koje je praktično nemoguće sve oboriti. Dva proizvoda koja mogu pomoći tako što će zaštiti vaše javne veb sajtove su Cloudflare i Google Project Shield.

Korak 3: Pristup i upravljanje nalozima

Jedan od najizazovnijih aspekata bezbednosti jeste onemogućavanje pristupa neovlašćenim licima. To znači sprečavanje protivnika da steknu pristup vašim podacima i onemogućavanje pristupa osobama unutar vaše kampanje informacijama koje im nisu potrebne. Mada se neke od preporuka dole mogu učiniti opterećujućim, uspeh hakera zavisi od onih koji prednost daju pogodnosti umesto bezbednosti.

ŠTA JE DVOSTEPENA AUTORIZACIJA?

Dvostepena autorizacija predstavlja dodatni nivo bezbednosti koji podrazumeva da korisnik obavi dodatnu potvrdu svog identiteta uz korišćenje svoje lozinke. Drugi stepen je od kritične važnosti jer, u slučaju da je vaša lozinka ukradena, protivnik se i dalje ne može prijaviti na vaš nalog. Vaša lozinka je nešto što vi znate, a drugi stepen bezbednosti je nešto što imate, poput šifre koju generiše neka aplikacija, fizičkog ključa ili čak biometrijskog faktora kao što je to otisak prsta.

DOBAR NIVO BEZBEDNOSTI — Šta treba da uradite

1. Uvedite verifikaciju u 2 koraka (2FA) na svim sistemima i aplikacijama. Izbegavajte verifikaciju u 2 koraka putem tekstualnih poruka (SMS) jer hakeri lako mogu klonirati telefonski broj i steći pristup tekstualnim porukama. Postoji nekoliko aplikacija za verifikaciju u 2 koraka koje funkcionišu jednako dobro kao tekstualne poruke, a to su Google Authenticator, Microsoft Authenticator i Duo Mobile. Možete takođe koristiti fizički ključ za „brzu identifikaciju na internetu“ (fast identity online - FIDO) koji se postavlja na vaš USB disk kao što su to Yubikey ili Feitian. Veb sajt „TwoFactorAuth.org“ je koristan vodič za servise koji nude i koji ne nude verifikaciju u 2 koraka.
2. Lozinke.
    a. Postavite kao uslov korišćenje jakih lozinki. Kao što smo to naznačili ranije, „kreirajte lozinke koje su dugačke i jake“. Današnji računari mogu dešifrovati lozinku od sedam znakova za nekoliko milisekundi. Za lozinku koja se sastoji od 20 ili čak 30 znakova biće potrebno znatno više vremena za dešifrovanje. Izaberite niz reči koje lako možete zapamtiti.
    b. Ne ponavljajte lozinke! Koristite različite lozinke za različite naloge kako haker ne bi mogao pristupiti većem broju naloga ako ukrade samo jednu lozinku.

c. Da biste zaštitili osoblje kampanje i volontere od „pecaroških“ napada, delite lozinke s kolegama samo u kontaktu licem u lice ili putem samouništavajućih šifrovanih poruka. Postavite kao uslov resetovanje lozinki za centralne naloge koje će se dobijati korišćenjem ovih istih metoda ili preko konferencijskih video poziva kako biste se uverili da je to zaista član osoblja ili volonter u kampanji. Nikada ne delite lozinke putem elektronske pošte, niti ih skladištite/distribuirajte putem servisa za pomoć korisnicima.

3. Koristite program za upravljanje lozinkama kao što su to LastPass, 1Password ili Dashlane koji će vam pomoći da lako upravljate većim brojem dugačkih i jakih lozinki. No postarajte se da vaš sistem za upravljanje ima dugačku, jaku lozinku i verifikaciju u 2 koraka. Trenutno ne preporučujemo programe za upravljanje lozinkama ugrađene u pretraživače interneta kao što su to Chrome, Safari i Firefox, koji su često manje bezbedni od samih programa za upravljanje lozinkama.

4. Kreirajte odvojene naloge za administratore i korisnike, i značajno ograničite pristup administratorskim nalozima. Administratori bi trebalo da imaju dva odvojena naloga za kampanju—jedan koji bi se koristio samo za njihove administratorske dužnosti i drugi koji bi bio njihov standardni korisnički nalog za sve ostale poslove u kampanji. To će smanjiti verovatnoću da neki protivnik bude u mogućnosti da ugrozi administratorski nalog koji bi omogućio pristup celokupnoj mreži.

5. Iznova periodično razmotrite ko ima pristupa različitim uređajima i mrežama. Odmah blokirajte pristup osoba koje napuštaju kampanju. Odmah promenite lozinke ako se uoči sumnjiva aktivnost. Da biste to omogućili, postarajte se da vaše osoblje ne deli korisničke naloge.

PROGRAMI ZA UPRAVLJANJE LOZINKAMA

Programi za upravljanje lozinkama predstavljaju način za skladištenje, povraćaj zaboravljenih i generisanje novih lozinki. Neki čak imaju mogućnost automatskog popunjavanja polja za unos lozinke na stranicama za prijavu. Program za upravljanje lozinkama i sâm koristi lozinku za prijavljivanje u program, ali to onda postaje jedina lozinka koju morate zapamtiti. Rizik je, naravno, da ukoliko neko izvrši upad u vaš program za upravljanje lozinkama (to se dešavalo!) ta osoba će steći pristup svim vašim lozinkama. Ipak, prednosti jakih, jedinstvenih lozinki na svim vašim nalozima skoro uvek znatno nadmašuju rizik koji se može bitno smanjiti korišćenjem dvostepene autorizacije kod pristupa vašem programu za upravljanje lozinkama. U kampanjama, programi za upravljanje lozinkama ponekad imaju smisla za višekorisničke naloge jer administratori mogu bezbedno podeliti pristup nalogu među njima.

UNAPREĐEN NIVO BEZBEDNOSTI — Preduzmite sledeći korak

1. Kreirajte korisničke profile za različite kategorije osoblja kampanje kojima se automatski dodeljuje neophodan nivo pristupa. Različitim vrstama zaposlenih—volonterima, pripravnicima, osoblju na terenu, rukovodstvu kampanje—potreban je pristup različitim resursima. Unapred utvrđeni profili olakšavaju dodelu nivoa pristupa čime se obezbeđuje da članovi osoblja stiču samo onu vrstu pristupa koja im je potrebna.

ŠTA SU ADMINISTRATORI?

U „informatičkom žargonu“, „administrator“ ili „admin“ može da ljudima omogući pristup ili kontrolu nad sistemima ili informacijama. Na primer, kao „admin“ za sistem elektronske pošte, možete kreirati naloge, menjati lozinke i postaviti uslove poput dužine lozinke i dvostepene autorizacije za sve naloge. U kancelarijskom programskom paketu kao što su GSuite ili Microsoft 365, takođe možete kreirati grupe kao što su „terenski tim“ ili „komunikacijski tim“. Posao admina je zaista važan. Ako sve urade kako treba, informacije će biti dostupne samo osobama kojima su potrebne, što je od suštinskog značaja za bezbednost. To znači da je odlučivanje o tome ko dobija administratorska ovlašćenja takođe odluka od kritične važnosti. Samo nekoliko obučenih osoba od velikog poverenja bi trebalo da drugima omogućava pristup informacijama. Ako član osoblja s „admin“ ovlašćenjima napusti kampanju, pobrinite se da im se odmah oduzmu ovlašćenja!

Korak 4: Planiranje reagovanja na incident

Planirati reakciju na napad jednako je važno kao što je izrada bezbednosne strategije da bi se napad sprečio. Kako reagovati je često u većoj meri povezano s konačnim ishodom incidenta nego s onim što je ugroženo. Treba odvojiti vreme da viši rukovodioci ili uprava rasprave šta će se desiti ako nešto pođe naopako. Evo liste za proveru koraka koje treba preduzeti:

PRAVNI Korak

Identifikujte spoljnog savetnika kome ćete se obratiti u slučaju visokotehnološkog napada i raspravljajte o procesu reagovanja na napad s njim na početku kampanje. U većini slučajeva, to će biti ista osoba koja zastupa vašu kampanju po drugim pitanjima, ali idealno bi bilo da imate nekoga ko se specijalizovao za reagovanje na incident po pozivu, bilo *pro bono* ili za $0 naknade.

Zamolite vašeg advokata da objasni pravne obaveze ako se podaci ukradu i koje mere morate imati uvedene da bi sve bilo u skladu s propisima.

Budite upoznati s pravnim obavezama vaših dobavljača informatičke opreme i usluga da vas obaveste ako dođe do hakerskog upada. Kad god je to moguće, unesite stroge uslove o obaveštavanju u vaše ugovore s dobavljačima pošto su treće strane čest izvor hakerskih upada.

Ako verujete da je vaša bezbednost narušena, najbolja praksa jeste da vaš advokat nadgleda vašu reakciju po osnovu poverljivog odnosa između advokata i klijenta.

Razgovarajte s vašim advokatom o najboljem načinu za saradnju s policijom ako do narušavanja bezbednosti dođe. Svaka kampanja će imati drugačiji pristup tome.

TEHNIČKI Korak

Utvrdite unapred koga ćete pozvati za pružanje tehničke pomoći ako mislite da je došlo do hakerskog napada.

Izaberite nekoga unutar kampanje ko će se povezati s tehničkim ekspertima u slučaju hakerskog upada. Idealno bi bilo da to bude ista osoba koja je već zadužena za informatičku koordinaciju za potrebe kampanje. Upravljanje reagovanjem na incident može biti veoma zahtevno tako da želite nekoga usredsređenog na tehničke aspekte ko zna šta radi. U tom slučaju se vi možete usredsrediti na komunikaciju sa zainteresovanim stranama i medijima.

Upoznajte se s tehničkom pomoći i drugom vrstom podrške koju vam pružaoci platforme mogu dati u slučaju incidenta poput hakerskog upada ili druge vrste napada.

OPERATIVNI Korak

Odlučite unapred ko će biti u vašem timu za reagovanje na incident i ko će biti na sastancima posvećenim reagovanju kampanje na incident. Važno je uključiti nekoga iz vašeg informatičkog, pravnog, operativnog i komunikacijskog tima. Ako ste mala kampanja i nemate komunikacijsku, informatičku ili operativnu podršku s punim radnim vremenom, planirajte da uključite ključno osoblje koje nadgleda aktivnosti kampanje.

Utvrditi lanac komande za donošenje odluka u slučaju hakerskog upada, pogotovo u pogledu komunikacija. U mnogim slučajevima, to će biti rukovodilac kampanje, ali neki rukovodioci kampanje bi mogli odlučiti da delegiraju odgovornost nekom drugom.

Identifikujte koju ćete aplikaciju ili tehnologiju koristiti za komunikaciju ako mislite da su vaši sistemi ugroženi. Na primer, ako su hakeri upali u vašu elektronsku poštu, možda ćete želeti da se oslonite na aplikacije za bezbednu razmenu poruka kao što su to Signal ili Wickr. Komunikacija za vreme trajanja upada je od suštinske važnosti, ali ne želite da vaši protivnici znaju o čemu razgovarate—ili čak da reagujete na njihove akcije.

KOMUNIKACIJSKI Korak

Isplanirajte scenarije. Za mnoge kampanje, to može biti deo postojećeg strateškog odstupanja. Za veće kampanje kojima preti veći rizik, možda će biti neophodno da se održi sastanak posvećen tome.

Identifikujte ključne unutrašnje i spoljne aktere, poput vašeg osoblja, volontera, donatora i pristalica. Treba da znate koga treba kontaktirati ako dođe do incidenta i rangirajte ih redom prema prioritetima. Izradite listu kontakata i odredite ko će stupiti u kontakt s njima.

Pretresite scenarije u kojima trpite najveću štetu i razmotrite kako se vaši akteri i poruke mogu promeniti u svakom od njih. Različiti scenariji bi mogli obuhvatiti sledeće:

- glasine da je vaša kampanja doživela hakerski upad;
- da su informacije na osnovu kojih se lično mogu identifikovati vaše pristalice procurile;
- da su osetljive finansijske informacije o donatorima ukradene, poput brojeva kreditnih kartica i kontakt informacija;
- ucenjivački softver (ransomware) je ubačen u vašu kampanju i došlo je do pokušaja iznude;
- vaši sistemi su obrisani i oboreni;
- nečija elektronska pošta je ukradena;
- vaš protivnik je ukrao vaša administratorska ovlašćenja i sve datoteke s čvrstog diska vaše kampanje;

> vaši nalozi na društvenim medijima su oboreni ili je došlo do hakerskog upada;
>
> internet je blokiran, ili su pojedini sajtovi, aplikacije ili protokoli blokirani u čitavoj zemlji;
>
> pristup kritičnim informacijama je blokiran ili onemogućen zbog cenzure.

> Pretresite scenarije u kojima trpite najveću štetu i razmotrite kako se vaši akteri i poruke mogu promeniti u svakom od njih. Različiti scenariji bi mogli obuhvatiti sledeće:

Budite obazrivi u pogledu toga što sada govorite o politici visokotehnološke bezbednosti ili incidentima. Neke žrtve visokotehnološkog kriminala su ranije davale grandiozne izjave o sopstvenim merama bezbednosti ili su kritikovale druge koji su bili meta napada. Mediji će tražiti od vas da položite račune za one što ste rekli u prošlosti ukoliko postanete žrtva hakerskog napada.

Takođe izbegnite iznošenje detalja o razmerama incidenta u njegovim ranim fazama (ako možete izbeći da uopšte govorite o razmerama incidenta, utoliko bolje). Detalji koji su dostupni na početku će se menjati kako napreduje istraga o incidentu. Uobičajena je greška izjaviti nešto što se naknadno pokaže kao netačno (npr. „nisu nam ukrali puno toga“ ili „nisu ukradeni lični podaci“). Najsigurnije je reći samo ono što sigurno znate. Izjave bi trebalo da se usredsrede na radnje koje preduzimate da biste zaštitili aktere pogođene hakerskim napadom.

Pripremite neke uopštene fraze unapred, a idealno bi bilo da to učinite uz konsultacije s vašim pravnim zastupnicima kako biste mogli da sročite izjave ili elemente za izjave brzo ako do incidenta dođe. Minimum bi bio da izradite jednostavan dokument s pitanjima i odgovorima koji možete brzo revidirati ako bude uopšte potrebe da ga upotrebite. Izrada dokumenta s pitanjima i odgovorima unapred će vam pomoći da razmislite o tome šta nećete reći jednako kao i o onome što ćete reći. Na primer, prvo pitanje će često biti: „Šta se desilo?“ Međutim, možda nećete biti u mogućnosti da na to pitanje odgovorite danima ili nedeljama. Činjenica da ne znate do koje vrste upada je došlo vam zapravo može pomoći da napišete bolje uopštene odgovore unapred.

PITANJA KOJA TREBA DA UKLJUČITE U VAŠ DOKUMENT S PITANJIMA I ODGOVORIMA SU:

- Šta se desilo?
- Kako se to desilo?
- Ko je to uradio?
- Šta je ukradeno ili oštećeno?
- Da li su ukradeni lični podaci bilo koga? Šta činite da biste ih zaštitili?
- Kako su to hakeri uradili?
- Da li su hakeri sada izvan vašeg sistema?
- Koliko su dugo bili u vašem sistemu?
- Koje ste bezbednosne mere primenili? Zašto nisu bile delotvorne?
- Zar nije trebalo da znate da se to može dogoditi? Zašto vaši sistemi nisu bili bolje obezbeđeni?
- Da li sarađujete s policijom? Da li vas je policija kontaktirala?
- U slučaju napada ucenjivačkim softverom, pitaće vas: „Da li ste platili otkup i zašto, ili zašto niste?“

Ostanite u kontaktu s vašim ključnim akterima i obaveštavajte ih koliko god je to moguće. Verovatno nećete moći da kažete puno toga, ali ključno je da ih kontaktirate redovno i obaveštavate o onome što znate, da imate jasnu izjavu o vašim namerama i da dajete detalje o onome što preduzimate da biste upravljali novonastalom situacijom. Izbegnite postavljanje praga očekivanja visoko gde bi se najnovije vesti s vaše strane očekivale isuviše često jer obično nećete imati novih informacija, a vaši akteri će postati isfrustrirani ako im se javljate bez najnovijih vesti. Medijima se obraćajte jedino proaktivno ukoliko imate nove informacije koje im možete dati.

Korak 5: Uređaji

Svaki fizički uređaj u kampanji—od mobilnog telefona, preko tableta i laptopa ili rutera, do štampača i kamere—predstavlja potencijalnu tačku upada u vašu mrežu. U sklopu dobrog plana visokotehnološke bezbednosti pokušaće se da se kontroliše pristup svim uređajima. Možete kontrolisati pristup uređajima tako što ćete se postarati da se njima rukuje valjano i da se uvek zna gde su. Pristup uređajima kontrolišete putem dvostepene autorizacije i jakih lozinki. Sadržaj na uređajima kontrolišete putem enkripcije i politika koje vas usmeravaju kako da skladištite podatke (tj. skladištenje informacija u oblaku umesto na uređajima).

DOBAR NIVO BEZBEDNOSTI — Šta treba da uradite

1. Uvek koristite poslednju verziju operativnog sistema (OS) koja je dostupna pošto ažuriranja sistema obuhvataju zakrpe za nedavno otkrivene ranjivosti sistema. Ako je to moguće, podesite uređaje da se automatski ažuriraju. Neka nečiji posao bude da redovno proverava da li su operativni sistemi na svim uređajima ažurni.

2. Izrađujte rezervne kopije! Za sve podatke koje čuvate na lokalnom uređaju (vašem računaru, na primer) se pobrinite da postoji plan za izradu rezervnih kopija korisničkih podataka u slučaju fizičke krađe, u slučaju da vam se računar pokvari ili da prospete kafu preko tastature. Na primer, možete koristiti uslugu automatske izrade rezervne kopije podataka u oblaku kako biste ublažili uticaj gubitka podataka na uređaju. Možete koristiti, recimo, Backblaze i CrashPlan.

3. Pristup uređaju

    a. Od početka, rukovodstvo kampanje bi trebalo da stvori okruženje u kome svi shvataju fizičko obezbeđenje svojih uređaja ozbiljno—gubitak uređaja bi protivniku mogao omogućiti pristup kritičnim informacijama koje se mogu upotrebiti da se nanese šteta kampanji.

    b. Mada mnoge kampanje ne mogu priuštiti kupovinu novih uređaja, uvek je najbolje kupiti novu opremu (pogotovo računare i telefone) ako možete. Minimalno bi trebalo pribaviti nove uređaje za osoblje koje radi na osetljivim podacima ili bi minimalno trebalo obrisati i ponovno instalirati operativni sistem na tim starim uređajima. Ako osoblje koristi sopstvene računare i telefone, ustanovite politiku koja se zove „donesi sopstveni uređaj“ (BYOD) u sklopu koje se primenjuju stroge bezbednosne prakse (vidi zaštitu na krajnjim tačkama sistema dole).

    c. Članovi osoblja kampanje NE bi trebalo da koriste lične naloge elektronske pošte koji nisu obezbeđeni shodno politici „donesi sopstveni uređaj“ za poslove u kampanji, uključujući elektronsku poštu i društvene medije. Svaka važna informacija koja se nalazi izvan uređaja

ili sistema koje se kontrolišu unutar kampanje je ranjiva na napad. Rukovodstvo bi trebalo da neprestano naglašava kako bi podaci iz kampanje trebalo da ostanu izvan lične elektronske pošte i neobezbeđenih računara.

d. Vodite računa o fizičkoj bezbednosti vaših uređaja. Kada koristite javni prevoz, ili ste u kafeu, čak i kada ste u kancelariji, uvek preduzimajte korake za sprečavanje krađe vaših uređaja što bi omogućilo pristup vašim nalozima, prepisci i podacima.

e. Odmah izvestite o izgubljenim uređajima. Postavite kao uslov podešavanje koje omogućava daljinsko brisanje sadržaja na svim uređajima. Za to, na primer, možete koristiti Find my iPhone i Android Device Manager.

f. Bez obzira da li ste pobedili ili izgubili na izborima, imajte pripremljen plan za to što će se desiti sa svim podacima, nalozima i uređajima kada se kampanja okonča. Posebno je ranjiv period neposredno nakon završetka kampanje.

4. Pristup sadržaju na uređajima

a. Promenite fabričke lozinke i podešavanja svim uređajima. Mnogi uređaji pristižu od proizvođača s fabričkom lozinkom koju je zaista lako pogoditi. Takođe, onemogućite naloge za goste ako vam je uređaj dospeo u ruke s takvim nalogom.

b. Uključite opciju za automatsko zaključavanje mobilnih telefona i računara nakon dva minuta i postavite uslov da se mora uneti lozinka ili upotrebiti otisak prsta za otključavanje uređaja.

c. Uključite opciju automatskog brisanja sadržaja na vašim mobilnim uređajima kako bi sami obrisali sadržaj nakon određenog broja neuspešnog prijavljivanja.

5. Sadržaj na uređajima

a. Postavite kao uslov enkripciju na svim uređajima (računarima i mobilnim telefonima) kako biste se postarali da gubitak uređaja ne znači ugrožavanje sadržaja. Neki od programa za tu svrhu su FileVault za Mac OS i BitLocker za Windows. Neki uređaji, poput iPhone-a, imaju već fabrički podešenu tu opciju, ali to nije slučaj sa svim uređajima.

b. Instalirajte softver za zaštitu na krajnjim tačkama sistema na svim uređajima. Neki od takvih programa su, recimo, Trend Micro, Sophos i Windows Defender. Postoje posebne aplikacije za bezbednost na krajnjim tačkama sistema za mobilne telefone i tablete, poput aplikacije Lookout.

ŠTA JE ZAŠTITA NA KRAJNJIM TAČKAMA SISTEMA?

Krajnje tačke sistema su uređaji koje osoblje koristi, uključujući mobilne telefone, prenosive i stone računare. Oni su „krajnje tačke“ mreže unutar kampanje, a članovi osoblja su „krajnji korisnici“. Zaštita na krajnjim tačkama sistema centralizovano kontroliše i upravlja bezbednošću na udaljenim uređajima. Pogotovo je važno za kampanje koje dopuste osoblju da „donesu sopstvene uređaje“ (BYOD) da ti uređaji budu bezbedni, bez malicioznog softvera i da se mogu obrisati ako budu ukradeni ili izgubljeni. Putem zaštite na krajnjim tačkama sistema se takođe može pratiti da li je softver ažuriran i otkriti novi maliciozan softver ili potencijalne pretnje. Mnogim kampanjama se to može učiniti kao veliki napor koji treba uložiti, no ako to ugradite u vaš rutinski proces integrisanja osoblja u organizaciju i odvojite neko vreme za to unapred, uštedećete sebi puno nevolja kasnije.

UNAPREĐEN NIVO BEZBEDNOSTI — Preduzmite sledeći korak

6. Koristite softver za upravljanje mobilnim uređajima (mobile device management - MDM) pomoću koga pratite aktivnosti da biste obezbedili da svi uređaji budu u skladu s politikama bezbednosti za mobilne telefone i korisničke uređaje koje ste ustanovili za potrebe vaše kampanje. To su, na primer, VMware AirWatch, Microsoft InTune i JAMF. GSuite i Microsoft Office 365 takođe omogućavaju upravljanje mobilnim uređajima.

7. Koristite napredne servise za zaštitu od pretnji koje prate i javljaju vam o malicioznim aktivnostima, kao što su to CrowdStrike Falcon ili Mandiant FireEye. Crowdstrike ponekad nudi besplatno uslugu Falcon zaštite od upada u sistem putem Crowdstrike fondacije, zavisno od potreba vaše kampanje i finansijskih pravila primenjivih na vašu kampanju.

Korak 6: Mreže

Mreže su sistem fizičkog hardvera, digitalnog softvera i njihovih međusobnih veza. One predstavljaju još jedno okruženje u kome je mnogo potencijalnih meta za napade. Mrežna bezbednost obuhvata sve—od toga kako uređaji komuniciraju jedni s drugima do korišćenja usluga oblaka za skladištenje podataka.

DOBAR NIVO BEZBEDNOSTI — Šta treba da uradite

1. Skladištite podatke u oblaku u koji imate poverenja, a ne na ličnim računarima ili serverima. Svemu što je uskladišteno na ličnom uređaju preti veći rizik od hakerskog upada, krađe, nezgoda ili napada nego podacima uskladištenim u oblaku.
    a. Niko ne bi trebalo da ima pristup svim podacima na mreži; naloge sa sveobuhvatnim administratorskim pristupom ne bi trebalo koristiti u svakodnevnom radu. Podelite vaše skladište datoteka u zasebne fascikle i shodno tome odredite mogućnost pristupa.
    b. Pobrinite se da se pristup deljenom sadržaju omogućava samo putem pozivnice. Neki servisi upravljanja datotekama takođe dopuštaju određivanje datuma isteka važenja pozivnica i pristupa.
    c. Periodično revidirajte šta se deli i s kim.
2. Postavite zasebnu bežičnu (wi-fi) mrežu za „goste“, odnosno za posetioce i volontere, koja ograničava pristup resursima kampanje. Potrudite se da kupite rutere koji nude „profil za goste“ koji će automatski podeliti vašu mrežu. Naša je snažna sugestija da menjate lozinku za pristup mreži po okončanju svakog događaja u sklopu kampanje kada može doći do velikog odliva i zamene osoblja.
3. Kada putujete, ili pre nego što pripremite vaše kancelarije za kampanju, izbegavajte usluge javnih bežičnih mreža za pristup internetu koliko god je to moguće i koristite bežične mreže od poverenja gde god je to moguće. Ako vam je potreban pristup internetu preko mobilnih mreža, pokušajte da obezbedite osoblju kampanje uređaje mobilnih operatera za bežične hotspotove uz mogućnost povezivanja drugih uređaja na bežični hotspot. Javne bežične mreže za internet su često besplatne i lako je povezati se preko njih, ali napadači ih takođe mogu upotrebiti da prodru u vaš hardver.
    a. Gde je to moguće, osoblje bi trebalo da koristi servise virtualnih privatnih mreža (virtual private network - VPN). Virtualne privatne mreže vam pomažu da se zaštitite od uljeza kad ste povezani na javnu bežičnu mrežu za pristup internetu. Neki od VPN servisa su, recimo, ExpressVPN ili TunnelBear. Nisu svi VPN servisi isti. Čuvajte se besplatnih VPN servisa! Mnogi takvi servisi žele da se dokopaju vaših podataka!
4. Obezbedite vaš pretraživač interneta. Časopis „PC Magazine“ je proglasio Chrome i Firefox najbezbednijim pretraživačima interneta u 2017. godini. Bez obzira na to koji pretraživač interneta koristite, redovnog ga ažurirajte.

ŠTA SU VIRTUALNE PRIVATNE MREŽE?

Virtualna privatna mreža (VPN) je „tunel“ zaštićen enkripcijom za vaš internet saobraćaj, skriven od uljeza. Neke kancelarije ga koriste kao način za daljinsko prijavljivanje na kancelarijsku mrežu, ali to nije tako često u kampanjama. Kampanje bi trebalo da razmotre mogućnost da osoblje koristi virtualne privatne mreže na računarima ili mobilnim telefonima ako često moraju da koriste javne bežične mreže za pristup internetu ili mreže u koje ne možete imati poverenja (što je ponekad slučaj s osobljem koje putuje ili kancelarijama na terenu). Google je nedavno plasirao novi VPN sistem po metodu „uradi sam“ pod nazivom Outline.

UNAPREĐEN NIVO BEZBEDNOSTI — Preduzmite sledeći korak

1. Možete preduzeti naprednije korake za zaštitu vaše mreže, ali bi trebalo da njih sprovode informatički profesionalci. Sugerisali bismo vam da ih pitate da uključe sledeće korake:
    a. Postaviti hardverski zaštitni zid (firewall).
    b. Obezbedite vašu bežičnu vezu WPA2 ili 802.1x bezbednosnim protokolima za enkripciju (nemojte koristiti WEP).
    c. Konfigurisati veb proksi server u oblaku radi blokiranja pristupa sumnjivim sajtovima od strane bilo kog uređaja koji pripada kampanji, bez obzira gde se nalazi. Pružaoci ovakvih usluga su, između ostalih, Zscaler, Cisco Umbrella i McAfee Web Gateway Cloud Service.
    d. Skladištite vaše elektronske dnevnike aktivnosti (activity logs) kod pružaoca usluga oblaka kao što su to LogEntries ili SumoLogic.
    e. Segmentirajte vaše skladište podataka u oblaku tako da nisu svi podaci smešteni na istom mestu. Istraživanja o političkim rivalima, strateške memorandume i podatke o osoblju bi trebalo čuvati u različitim fasciklama, a pristup tim fasciklama bi trebalo ograničiti na osobe kojima su uistinu potrebne. Razmotrite mogućnost korišćenja potpuno različitog sistema za skladištenje najosetljivijih podataka iz vaša kampanje. Ograničite pristup tako da ga ima samo ključno osoblje, i to samo kada koristi određene uređaje. (Na primer, ako koristite Microsoft365 kao vaš kancelarijski programski paket i za skladištenje dokumenata, smestite vaše najosetljivije dokumente na vaš Dropbox ili Box nalog.) Ako član osoblja vaše kampanje bude ugrožen napadom, ovakva segmentacija će limitirati štetu.
2. Obučite osoblje da ne povezuje svoje uređaje na nepoznate portove ili uređaje. Nemojte koristiti javne punjače na aerodromima ili na skupovima. Ne prihvatajte besplatne punjače ili baterije za mobilne telefone na događajima (taj besplatni USB disk može biti krcat malicioznim softverom!).

Korak 7: Informacione operacije i komunikacija okrenuta javnosti

Informacione operacije su se često pojavljivale u vestima nedavno, a pogotovo kampanje koje vode strane obaveštajne službe. Na izabranim liderima i kreatorima politika je da odluče kako će se suprotstaviti informacionim operacijama u budućnosti, a malo toga kao osoblje kampanje možemo učiniti da bi uticali na to da li će se desiti ili ne, no postoje neke stvari koje možemo uraditi da bismo upravljali našim odnosom prema njima, ako se dese. Kampanje jesu i biće mete takvih operacija i zato se treba pripremiti. Odbrana načina na koji vaša kampanja komunicira s javnošću je važan deo toga. Dole su neki načini za bolju zaštitu od informacionih operacija, identifikovanje trenutka kada utiču na vašu kampanju ili kandidata, i brzu reakciju na njih kada se dese.

ŠTA SU INFORMACIONE OPERACIJE?

Informacija je moć—ili makar to misle mnoge vojne i civilne obaveštajne službe! Moć ideja je dugo podstrekivala na pobunu, bunt i građanske ratove, i mnoge zemlje koje su možda u tradicionalnom vojnom smislu inferiorne teže korišćenju informacija da bi zavadile i zaokupile podelama svoje protivnike. U Rusiji, na primer, vršenje uticaja na javno mnjenje putem propagande i raspirivanja lokalnih tenzija je sastavni deo vojne doktrine i nešto je što upražnjavaju neprestano na onima koje percipiraju kao protivnike. Društveni mediji su u potpunosti promenili situaciju u pogledu informacionih operacija. Sada je lakše nego ikad brzo preneti informaciju i predstavljati se kao druga osoba, čime se stvara utisak o gnevu ili podelama u javnosti.

DOBAR NIVO BEZBEDNOSTI — Šta treba da uradite

1. Ne zaboravite da su informacione operacije komunikacijski, a ne tehnički problem. Protivnici mogu svoje informacione informacije učiniti potentnijim ako ukradu vaše podatke, ali nakon što informacije procure u šire okruženje, potrebna vam je komunikacijska strategija da biste se nosili s posledicama. Razmislite unapred kako postupati s lažnim ili iskrivljenim vestima. Da li ćete ih ignorisati? Da li ćete ih proslediti na Tweeter-u i naglasiti da se radi o lažnoj vesti? Kako ćete doneti ovu odluku? To su neke od najtežih odluka za svaku kampanju, ali

najvažnije je promisliti ova pitanja s vašim timom unapred kako bi vi i vaš tim imali smernice za reagovanje, ako uopšte budete reagovali.

2. Budite upoznati s tim što se dešava. Podstaknite aktiviste da dele postove, sajtove ili članke za koje utvrde da su sumnjivi. Ako želite, možete nekim pripravnicima ili volonterima dati zadatak da se konkretno na to usredsrede, da sprovode pretrage kako bi pronašli kakvog sve sadržaja ima. Jedan aktuelan izazov jeste to što je nemoguće videti sve što glasači dobijaju na svojim Facebook fidovima. Ova platforma je otežala postavljanje političkih oglasa i povećala je broj osoblja koje prati informativni sadržaj, no ne možete pretražiti celokupan sadržaj. Najbolji način za rešavanje ovog problema sada jeste da date zadatak timu volontera koji predstavljaju različite geografske odrednice i demografske grupe u vašoj zemlji/okrugu kako biste „ulovili“ što više sumnjivog sadržaja.

3. Uspostavite kontakt s ključnim platformama društvenih medija i obavestite ih ako pronađete lažnu ili pogrešnu informaciju. Većina platformi društvenih medija će sada ukloniti „lažan“ ili pogrešan sadržaj, kao i profile varalica. Zatražite od vašeg relevantnog odbora kampanje ili stranke na nacionalnom nivou najbolje kontakte za platforme društvenih medija i stupite u kontakt s njima u ranoj fazi kampanje kako biste mogli da im se brzo obratite ako nešto pođe naopako.

    a. Facebook

    b. Twitter

    c. Google/Youtube

4. Pratite sajtove varalica. Danas nema javnih izveštaja o varalicama koje pokušavaju da vam ukradu novac ili podatke aktivista preko svojih lažnih veb sajtova, ali to je tako lagan metod napada da bi trebalo da budete na oprezu. Postarajte se da kupite svaku web adresu koju biste poželeli da koristite (inače će biti iskorišćena protiv vas). Ako želite, možete koristiti servis upravljanja reputacijom koja će pratiti sadržaj na internetu za vas. Neki servisi pružaju tu uslugu po prilično niskoj ceni.

5. Zaštitite se od napada putem distribuiranog uskraćivanja pristupa (poznatog kao DDoS). DDoS napad se dešava kada protivnik preuzme kontrolu nad puno uređaja i koristi ih da istovremeno sa svih njih „pinguje“ vaš veb sajt što dovodi do rušenja sajta. Uglavnom se u ovom vodiču usredsređujemo na to kako na odstojanju zadržati ljude od podataka iz vaše kampanje, ali, u slučaju DDoS-a, vi želite da vaš veb sajt ostane otvoren i dostupan sve vreme za vaše donatore i aktiviste. DDoS još uvek nije postao uobičajena pretnja predizbornim kampanjama, ali bi se mogao iskoristiti da vas spreči da prikupljate sredstva ili prosto da dovede do uistinu frustrirajućeg ometanja vaše kampanje. Postoje dve besplatne alatke koje možete koristiti za zaštitu vašeg veb sajta, Google Shield i Cloudflare.

Da li mislite da se ovaj priručnik može učiniti boljim?

Ima li novih tehnologija ili ranjivosti kojima bi trebalo da se pozabavimo?

Želimo povratnu informaciju od vas.

Molimo vas podelite s nama vaše ideje, priče i komentare na Twitter-u @d3p koristeći heštag #CyberPlaybook ili nam pošaljite poruku elektronske pošte na connect@d3p.org da bismo nastavili da unapređujemo ovaj resurs kako se digitalno okruženje menja.

Projekat "O zaštiti digitalne demokratije"
Belfer Center za nauku i međunarodne odnose
John F. Kennedy School of Government
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/D3P